SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

ACCOUNTING IN PEER-TO-PEER DATA COMMUNICATION NETWORKS

Cross Reference to Related Applications

PRIORITY STATEMENT UNDER 35 U.S.C.119(e) & 37 C.F.R.S.1.78. This non-provisional patent application claims priority based upon the prior U.S. provisional patent application entitled "Software Deployment, Accounting and Personal Portal", application number 60/287,734 filed May 2, 2001, in the name of GONTHIER Jean-Charles, RICHER Eric, HOST Gerald, JODOIN Pierre-Luc, FOURNIER Nicolas, MALTAIS Robert Claude, VAN BUNNINGEN Thomas, HARNOIS Serge, WALLNER Sabine, BRASK Patrik

Background of Invention

[0001] Technical Field of the Invention

[0002] The present invention relates to data communications networks, and particularly to accounting in such networks.

[0003] Description of Related Art

[0004] Peer-to-Peer networks are networks in which each network element (peer), such as for example a user device or a server, can communicate directly with other network elements. For example, instead of sending mail to a mail server and then have the recipient download it, a peer would send the mail directly to the recipient without intermediary (other than routers and the like).

[0005] To the present day, Peer-to-Peer networks have been used in trusted environments, such as for example in a local network where network access is only allowed from a number of known devices. User authentication is unnecessary in such a trusted network,

and since there is no user authentication accounting is impossible as there is know way of knowing who used a certain service. This usually is no big problem, since the peers in a trusted environment either do not expect to be paid for the services they provide or are paid by the network administrator that for instance may charge the peers a flat fee.

[0006] In an open network environment, i.e. a network that is accessible by "anyone", service providers usually expect to be paid for the services they provide. In these open networks, the users must be authenticated in order for real accounting for the use of services to be possible. Furthermore, peers that provide a service often have no own means to perform authentication and accounting.

[0007] It can therefore be appreciated that there is a need for a solution that overcomes the problems and limitations of the prior art by providing secure charging. This invention provides such a solution.

Summary of Invention

[0008] The present invention is directed to a method for charging in a data communications network comprising a User, a Service Provider that provides at least one service, and an Accounting Manager. The Accounting Manager sends a service credential to the User and a user credential to the Service Provider. The User requests a service from the Service Provider that validates the request. The service is then initiated. After that, the Service Provider sends an accounting message to the Accounting Manager.

[0009] The present invention is further directed to a system for charging in a data communications network. The system comprises a User, a Service Provider that provides at least one service, and an Accounting Manager. The Accounting Manager sends a service credential to the User and sends a user credential to the Service Provider. The User requests a service from the Service Provider using information from the service credential, and the Service Provider validates the request and sends an accounting message to the Accounting Manager.

[0010] The present invention is further directed to a User node in a data communications network further comprising a Service Provider and an Accounting Manager. The User node comprises a communication unit that receives a service credential from the Accounting Manager and requests a service from the Service Provider.

[0011] The present invention is further directed to an Accounting Manager in a data communications network further comprising a User and a Service Provider. The Accounting Manager comprises a communication unit that sends a service credential to the User, sends a user credential to the Service Provider, and receives an accounting message from the Service Provider.

[0012] The present invention is further directed to a Service Provider providing at least one service in a data communications network that further comprises a User and an Accounting Manager. The Service Provider comprises a communication unit that receives a user credential from the Accounting Manager, receives a request for a service from the User, and sends an accounting message to the Accounting Manager.

[0013] The present invention is further directed to a system for charging in a data communications network that further comprises a User. The system comprises a Service Provider that provides at least one service, and an Accounting Manager. The Accounting Manager is sends a service credential to the User, sends a user credential to the Service Provider, and receives a request for a service from the User. The Service Provider validates the service request, using information from the user credential, and sends an accounting message relating to the service to the Accounting Manager.

Brief Description of Drawings

[0014] A more complete understanding of the present invention may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0015] FIG. 1 depicts a block chart of an exemplary network environment in which the invention may be used;

[0016] FIG. 2 depicts a signal flow chart of a preferred embodiment of the method according to the invention; and

[0017] FIG. 3 depicts a simplified block chart of an exemplary network node.

Detailed Description

[0018] Reference is now made to the Drawings, where Figure 1 depicts a block chart of an exemplary network environment in which the invention may be used. In the network 20,

is shown a User 22 connected to the Internet 10 through an access network 12. The User 22 may be a person using some kind of device to interface with the network or it may be an intelligent device. The User 22 may have an Internet portal 23 (hereinafter called portal) or other interface through which the User 22 can use services and browse for information. It is preferable if the User 22 has logged on to the portal 23 so that the portal 23 may act in the User"' 22 name directly without having the User 22 authenticate himself for example every time a service is to be used. The portal 23 itself is however beyond the scope of this invention.

[0019] There is further a Service Provider 24, with a direct connection to the Internet 10, that is willing to provide services detailed in a first service list 25 to the User 22 for money. The network 20 further comprises an Accounting Manager 26, also with a direct connection to the Internet 10, that among other things is in charge of accounting for at least the services detailed in a second service list 27 that it may provide to the User 22 that may store it as service list 27", as will be further described hereinafter. There is also an Accounting Storage 28 in which accounting data are stored. The Accounting Storage 28 is connected to the Accounting Manager 26, in this case directly, but they may also be interconnected via the Internet 10 or be co-located.

[0020] In an exemplary scenario, the User 22 wishes to use a service provided by the Service Provider 24. The service may for example be a stock analysis or a game and the Service Provider 24 is willing to let the user partake of the service for a fee that for example may depend on the length of the utilisason.

[0021] Figure 2 depicts a signal flow chart of a preferred embodiment of the method according to the invention. This method allows a user to request and use a service provided by a peer, and also allows proper accounting. The figure shows, in a network 20 comprising for example the Internet (10 in Figure 1), the User 22, the Service Provider 24, the Accounting Manager 26 and the Accounting Storage 28.

[0022] It will be assumed that both the User 22 and the Service Provider 24 each have a valid security association, also called a trust relationship, with the Accounting Manager 26.

[0023]

A security association is one way to authenticate an entity in a network. This may for instance be a shared secret that no one else knows about. When one entity wants to

authenticate another entity it asks for their shared secret and if the response comprises the correct secret, then the other entity is authenticated. An example of such a secret is an encryption key. The first entity draws a random number and sends it to the second entity. Both entities encrypt the number using their shared encryption key. The second entity sends the encrypted number to the first entity that then is able to compare the two encrypted numbers. Encrypting random numbers is a way to make sure that a third entity may not learn the shared secret, as the secret is not the number itself nor its encrypted version, but rather the encryption key per se.

[0024] Another example is public key encryption (PKE) where an entity has a private key that only the entity itself knows and a public key that may be known to the entire world. A message encrypted with the public key may only be decrypted with the corresponding private key, and vice versa. Hence, a message encrypted with the private key may be said to have been signed by the corresponding entity; an electronic signature so to speak. This way an entity that only knows the public key of one entity, may ask that entity for the public keys of other entities. Thus, two entities that previously did not know each other's public keys may gain knowledge of this, usually through an entity they both trust.

[0025] A person skilled in the art will appreciate that these were merely two examples of security associations and that other variants exist.

[0026] It will further be assumed that the Accounting Manager 26 has a list (27 in Figure 1) of services that it supports, i.e. that it among other things provides accounting for.

[0027] The Accounting Manager 26 already has, perhaps during a previous session, provided the User 22 with a list of available services (27" in Figure 1).

[0028] The User 22 is able to communicate with the Service Provider 24 and the Accounting Manager 26 through an interface, such as for example the portal 23 shown in Figure 1, or a, possibly mobile, agent (not shown) acting on the User's 22 behalf.

[0029] Turning now to the description of the steps of the method according to the invention. The User 22 selects a service in the list of services, step 201, whereupon a Service Credential Request 202 is sent to the Accounting Manager 26. This Service Credential Request 202 comprises:

[0030] - An indication of the requested service. (a1)

[0031] - A unique identifier for the Service Credential Request 202. (a2)

[0032] - A random number to be used for authentication using the security association. (a3)

[0033] - An electronic signature that authenticates the User 22 to the Accounting Manager 26. (a4)

[0034] - A Certificate (e.g. according to the X.509 standard). (a5)

[0035] Upon reception of the Service Credential Request 202, the Accounting Manager 26 validates the former, step 204, and, if the validation was successful, responds with a Service Credential 206 that 206 comprises:

[0036] - The unique identifier from the Service Credential Request 202. (b1)

[0037] - The address of the Service Provider 24. (b2)

[0038] - A validity period or conditions for the use of the credential. (b6, b7)

[0039] - An electronic key that will allow the User 22 and the Service Provider 24 to authenticate one another. (b3)

[0040] - A unique accounting session identifier to be used for accounting for the User 22 for the particular use of the service. (b4)

[0041] - An electronic signature that authenticates the Accounting Manager 26 to the User 22. (b5)

[0042] The Accounting Manager 26 also sends a User Credential 208 to the Service Provider 24. The User Credential 208 comprises:

[0043] - The address of the User 22. (c1)

[0044] - The unique accounting session identifier to be used for accounting for the User 22 for the particular use of the service. (c2)

[0045] - An electronic key that will allow the User 22 and the Service Provider 24 to authenticate one another. (c3)

[0046] - An electronic signature that authenticates the Accounting Manager 26 to the Service Provider 24. (c4)

[0047] - Policies (c5) that specify under what conditions the User 22 may access the service, such as for example lifetime, time of day, maximum number of requests, and whether the user is allowed to change his address. In addition, there are accounting policies such as for example the data that is to be collected and the maximum time between accounting messages.

[0048] The User 22 then sends a Service Request 210 to request the service from the Service Provider 24. This Service Request 210 comprises:

[0049] - The address of the User 22. (d1)

[0050] - The unique accounting session identifier. (d2)

[0051] - An electronic signature authenticating the User 22. The signature is built using the electronic key provided by the Accounting Manager 26. (d3)

[0052] The Service Provider 24 then validates the Service Request 210, step 211, using information from the User Credential. If the Service Request 210 is validated, the service is then initiated 212 by the Service Provider 24, the User 22, or by the Service Provider 24 and the User 22 together, and the service session begins. During the service session the content of any messages sent between the User 22 and the Service Provider 24 are specific to the service and fall outside the scope of the invention. However, these messages may comprise an electronic signature that authenticates them to the receiving entity.

[0053] In addition, depending on the configuration of the service and the accounting policies specified by the Accounting Manager 26, the Service Provider 24 may send one or more Interim Accounting messages 214 to the Accounting Manager 26. Each Interim Accounting messages 214 comprises:

[0054] - A unique identifier of the service. (e1)

[0055] - An indicator that the message comprises interim accounting data. (e2)

[0056] - The User Credential identifying the User 22. (e3)

[0057] - A unique accounting message identifier. (e4)

[0058] - Accounting data. (e5)

[0059] - The accounting session identifier. (e6)

[0060] - An electronic signature identifying the Service Provider 24 to the Accounting Manager 26. (e7)

[0061] Upon reception of an Interim Accounting message 214, the Accounting Manager 26 may respond with an Acknowledgement 216.

[0062] The User 22 or the Service Provider 24 may terminate the service session, step 218. Once the service is terminated, the Service Provider 24 sends to the Accounting Manager 26 a Final Accounting message 220 comprising:

[0063] - A unique identifier of the service.

[0064] - An indicator that the message comprises final accounting data.

[0065] - The User Credential identifying the User 22.

[0066] - A unique accounting message identifier.

[0067] - Accounting data.

[0068] - The accounting session identifier.

[0069] - An electronic signature identifying the Service Provider 24 to the Accounting Manager 26.

[0070] The Accounting Manager acknowledges the Final Accounting message 220 with an acknowledgement 221.

[0071] Every now and then, depending on pre-established policies agreed upon between the Accounting Manager 26 and the Accounting Storage 28, the former sends its stored accounting data to the latter in a Record Accounting message 222. Upon reception of this message, the Accounting Storage 28 stores the data and sends an Acknowledgement 224 to the Accounting Manager 26 that, upon reception of the Acknowledgement 224,

deletes, step 226, the accounting data it sent to the Accounting Storage 28 in the Record Accounting message 222.

[0072] Figure 3 depicts an exemplary network node such as for example an Accounting Manager 26. The network node 30 comprises a communication unit 31 for communication with other nodes in the network and a processing unit 32 for processing data. The network node also has a network address 33.

[0073] While the description illustrates a peer-to-peer network, it should be understood that the present invention also could be used in other kinds of networks.

[0074] Although several preferred embodiments of the methods, systems and nodes of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.